The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	NO. CR19-159 RSL **FILING IN ADVANCE OF STATUS CONFERENCE**

In addition to any other matters the Court wishes to address at the status conference scheduled for May 25, 2022, in this case, the government asks that the Court address two specific subjects. First, the government asks that the Court conduct an inquiry of Defendant, Paige Thompson (either *ex parte*, or in open court), and ask that Thompson waive, on the record, a possible conflict with her counsel stemming from the fact that one or more of her counsel may be victims of the crimes with which Thompson is charged. Second, if necessary, the government asks that the Court schedule a hearing the week prior to trial to address any issues regarding the authenticity of various business and electronic records, for which the government has provided notice pursuant to Federal Rule of Evidence 902(11), (13) and/or (14), that may still be outstanding.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I. THE POSSIBLE CONFLICT OF INTEREST

A. Facts

Defendant, Paige Thompson, is charged in this case with hacking into servers of numerous companies that used cloud computing services provided by Amazon Web Services (AWS) and stealing information from those companies. Among the companies from which Thompson stole information is Capital One Financial Corporation ("Capital One").

The information Thompson stole from Capital One includes information from credit card applications submitted to Capital One by approximately 106 million people. In most instances, much of the most sensitive information (such as Social Security numbers and bank account numbers) was encrypted, and therefore not actually available to Thompson. But other information, such as applicants' names, dates of birth, partial addresses, and self-reported income was not encrypted. And, in a small percentage of cases (in the hundreds of thousands), information about Social Security numbers and/or bank account numbers was not encrypted.

The government's investigation to date suggests that the government recovered the only copy of the stolen data when it executed a search at Thompson's residence and seized Thompson's computer. Although Thompson threatened to "dump" (that is, disseminate) stolen data, the government has not developed evidence that Thompson ultimately did so. And, although Thompson appears to have taken steps toward using the stolen data to commit fraud—as evidenced, for instance, by the fact she conducted Google searches for terms like "credit card embosser" and "carding forums dark web" after stealing the information—the government has not developed clear evidence that she actually engaged in such financial fraud. The government has developed evidence that Thompson did use one person's information for some purpose, since her phone contained an autofill artifact for that person's name.

As noted in a previous filing in this case, based upon its recognition that members of the prosecution team might have a conflict of interest, the government consulted with

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Capital One to determine whether members of the prosecution team, or their spouses, had information stolen in this case. *See* Notice of Possible Conflict (Docket No. 171) (Sealed). According to Capital One, members of the prosecution team and/or their spouses had limited information stolen by Thompson, namely their names, dates of birth, partial addresses, and self-reported income. *See id.*

Based upon that information, and consistent with the provisions of the Justice Manual, the government consulted with the General Counsel's Office at the Executive Office of United States Attorneys (EOUSA). That office concluded that, given (1) the large number of victims (approximately 40% of the adult population of the United States), (2) the limited nature of the stolen information, and (3) the lack of particular impact on individuals at issue versus the general population, recusal was not required. *See id.*

The government did not ask Capital One to provide **i**nformation concerning defense counsel, in part because the government does not know the full roster of individuals working on the defense team, let alone their spouses' identities. The government did offer, in communications with defense counsel, and in its filing, to inquire of Capital One, or to facilitate defense counsel doing so. The government indicated in its filing that it believed that any conflict that defense counsel might have would be waivable, and that it would "work with defense counsel to ensure that they notify Thompson of such a possible conflict, and [] obtain an adequate waiver**."** *See id.* at 3.

Since its filing, the government repeatedly has asked defense counsel to agree to have Thompson waive, on the record, any possible conflict that members of her defense team might have due to the fact that Thompson is being prosecuted for stealing information that likely includes one or more members of the defense team's personal information (i.e., that they may be victims of her crime).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Defense counsel repeatedly have represented that they have addressed the conflict issue appropriately with Thompson, and the government has no reason to believe otherwise. Nevertheless, the government believes that the record should clearly reflect that Thompson is aware of the potential conflict, de minimus though it may be, and that she has agreed to waive any conflict that exists. Defense counsel does not believe any involvement by the Court—including any waiver on the record, including *ex parte*—is necessary or appropriate. A copy of the parties' last email exchange on the issue is attached as Exhibit 1.

B. Argument

It is well established that a criminal defendant has a constitutional right to the effective assistance of counsel. *Strickland v. Washington*, 466 U.S. 668, 686 (1984). Effective assistance of counsel means representation that is untrammeled and unimpaired, *Glasser v. United States*, 315 U.S. 60, 70 (1942), and requires representation by an attorney with undivided loyalty and free from conflicts of interest. *Strickland*, 466 U.S. at 688, *United States v. Partin*, 601 F.2d 1000, 1006 (9th Cir. 1979); *United States v. Williams*, 372 F.3d 96, 102 (2d Cir. 2005).

It also is well-established that the government has standing to raise the issue of opposing counsel's conflicts of interest with the court. *See, e.g.*, *United States v. Tatum*, 943 F.2d 370, 379-80 (4th Cir. 1991) (concluding that "when a conflict situation becomes apparent to the government, the government has a duty to bring the issue to the court's attention"). And, a trial court then has a responsibility "to investigate further, to advise the defendant personally, and to receive a knowing waiver if that is the expressed wish of the defendant." *Id.* at 379.

This is so, because of the interest in ensuring that defendants receive conflict-free representation. It also is true because "[c]onvictions are placed in jeopardy and scarce judicial resources are wasted" when conflict issues are not addressed in advance of trial, *United States v. Stantini*, 85 F.3d 9, 13 (2d Cir. 1996), and defendants subsequently are

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

able to challenge their convictions on the ground that they did not receive conflict-free representation.

In this case, the potential or actual conflict is relatively minor, given the massive number of victims (approximately 40% of the United States population) and the lack of apparent direct financial loss to those victims. Based on those facts, EOUSA authorized members of the prosecution team to prosecute the case, even though they had personally identifiable information (PII) stolen by Thompson. But there remains at least a potential conflict of interest on the part of the defense team (potential, because the defense team has not availed itself of the government's offer to learn whether any of its members' information was stolen), and there likely is an actual conflict for some members of the team.

The government believes this potential, or even actual, conflict is waivable. Although defense counsel have represented that they have addressed the issue appropriately, the Court should conduct a colloquy with Thompson to ensure, and create a record, that Thompson in fact is waiving any conflict knowingly, voluntarily, and intelligently. The government suggests that the Court do so during, or at the end of, the upcoming May 25, 2022, status conference. The government has no objection to defense counsel's request that any such colloquy be conducted *ex parte.*

II. RULE 902 CERTIFICATIONS

The Federal Rules of Evidence have established a process by which business records, records generated by electronic processes, and data copied from electronic storage media can be authenticated without the need to call foundational witnesses to authenticate them. This process is set forth in Federal Rule of Evidence 902(11), (13), and (14), respectively, for the three types of records. Those three sections provide that the following records are self-authenticating:

> **(11) Certified Domestic Record of a Regularly Conducted Activity.** The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

> proscribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record—and must make the record and certification available for inspection—so that the party has a fair opportunity to challenge them.
>
> . . .
>
> **(13) Certified Records Generated by an Electronic Process or System.** A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirement of Rule 902(11) or (12). The proponent must also meet the notice requirement of Rule 902(11)
>
> **(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Fed. R. Evid. 902. Assuming that a party has produced the relevant certification, and complies with the notice requirement, records are deemed authentic (and, so, admissible, provided they meet other evidentiary requirements, such as being relevant, non-hearsay, etc.).

As reflected in the Advisory Committee Notes to the 2017 Amendments to Rule 902, which enacted the latter two of these provisions,

> [a]s with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented.

Fed R. Evid. 902, Advisory Committee Notes, 2017 Amendments.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The government has followed this process in this case with respect to records produced in response to legal process during the investigation, by Twitter, Google, Slack, and GitHub. The last of these records were produced in discovery to defense in November 2020 (that is, a year-and-a-half ago), and most were produced substantially earlier than that. On May 16, 2022, the government sent a letter to defense counsel notifying them that it intended to rely upon Federal Rule 902(11), (13), and (14) to authenticate the documents. The government's letter, which is attached as Exhibit 2, identified the Bates number of the records, provided a description of the records, and identified the Bates number of the pertinent certifications from Twitter, Google, Slack, and GitHub.[1] Finally, the government's letter asked defense counsel to notify the government by the May 25, 2022, status hearing if defendant objected to the authenticity of any of these records.

The government has complied with all of the requirement of Federal Rules 902(11), (13), and (14) by obtaining certifications that comply with each of these rules, by providing written notice of intent to offer the records, and by providing both the records and the certifications to the defense. The government presumes that the defense will not object to the authenticity of the records (although, obviously, retaining the right to object on other grounds such as relevance or hearsay). If the defense has not provided confirmation of this fact by the time of the hearing set for May 25, the government will ask the court to set a hearing at any time convenient for the Court during the week of May 30-June 3, so that the defense can raise whatever challenge it has to the authenticity of the records, and the Court can rule on their authenticity. Failure to address the documents' authenticity in advance of trial would thwart Rule 902's purpose of avoiding inconvenience and expense on an issue (authenticity) concerning which the government is not aware of any legitimate dispute.

[1] The 902(11), (13), and (14) certifications themselves are attached as Exhibit 3.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

III. CONCLUSION

For the foregoing reasons, the government requests that the Court address the issues of Thompson's conflict waiver and the authenticity of Twitter, Slack, Github, and Google records at the May 25 status conference.

DATED: May 23, 2022.

Respectfully submitted,

NICHOLAS W. BROWN
United States Attorney

s/ Andrew C. Friedman
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CUBERTSON

Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Phone: (206) 553-7970
Facsimile: (206) 553-0882
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov
Tania.Culbertson@usdoj.gov